

ON DIRECTIONS DETERMINED BY SUBSETS OF VECTOR SPACES OVER FINITE FIELDS

ALEX IOSEVICH AND HANNAH MORGAN

This paper is dedicated to the memory of Nigel Kalton

ABSTRACT. We prove that if a subset of a d -dimensional vector space over a finite field with q elements has more than q^{d-1} elements, then it determines all the possible directions. If a set has more than q^k elements, it determines a k -dimensional set of directions. We prove stronger results for sets that are sufficiently random. This result is best possible as the example of a k -dimensional hyperplane shows. We can view this question as an Erdős type problem where a sufficiently large subset of a vector space determines a large number of configurations of a given type. See, for example, ([7]), [1], [4], [11], [12] and the references contained therein. For discrete subsets of \mathbb{R}^d , this question has been previously studied by Pach, Pinchasi and Sharir. See ([8]).

1. INTRODUCTION

The celebrated Kakeya conjecture, proved in the finite field context by Dvir ([2]), says that if $E \subset \mathbb{F}_q^d$, $d \geq 2$, contains a line (or a fixed positive proportion thereof) in every possible direction, then $|E| \geq cq^d$. Here, and throughout, $|E|$ denotes the number of elements of E and \mathbb{F}_q^d denotes the d -dimensional vector space over the finite field with q elements.

While Dvir's theorem shows that a set containing a line in every directions is large, in this paper we see to determine how large a set needs to be to determine every possible direction, or a positive proportion thereof. In the discrete setting the problem of directions was studied in recent years by Pach, Pinchasi, and Sharir. See [7] and [8]. In the latter paper they prove that if P is a set of n points in \mathbb{R}^3 , not all in a common plane, then the pairs of points of P determine at least $2n - 5$ distinct directions if n is odd and at least $2n - 7$ distinct directions if n is even.

Date: October 4, 2010.

This work was partially supported by the NSF Grant DMS10-45404. The article is based in part on Hannah Morgan's senior thesis at the University of Missouri-Columbia.

The authors wish to thank Doowon Koh, Steven Senger and Chun-Yen Shen for some helpful remarks and suggestions.

In order to state our main result, we need to make precise the notion of directions in subsets of \mathbb{F}_q^d .

Definition 1.1. We say that two vectors x and x' in \mathbb{F}_q^d point in the same direction if there exists $t \in \mathbb{F}_q^*$ such that $x' = tx$. Here \mathbb{F}_q^* denotes the multiplicative group of \mathbb{F}_q . Writing this equivalence as $x \sim x'$, we define the set of directions as the quotient

$$(1.1) \quad \mathcal{D}(\mathbb{F}_q^d) = \mathbb{F}_q^d / \sim.$$

Similarly, we can define the set of directions determined by $E \subset \mathbb{F}_q^d$ by

$$\mathcal{D}(E) = E - E / \sim,$$

where

$$E - E = \{x - y : x, y \in E\},$$

with the same equivalence relation \sim as in (1.1) above.

It is not difficult to see that $|\mathcal{D}(\mathbb{F}_q^d)| = q^{d-1}(1 + o(1))$. Thus the question above is rephrased in the following form. How large does $E \subset \mathbb{F}_q^d$ need to be to ensure that $\mathcal{D}(E) = \mathcal{D}(\mathbb{F}_q^d)$, or, more modestly, that $\mathcal{D}(H_n) \subset \mathcal{D}(E)$, where H_n is a n -dimensional plane.

Since E may be a k -dimensional plane, a *necessary* condition for $\mathcal{D}(H_{k+1}) \subset \mathcal{D}(E)$ is $|E| > q^k$. We shall see that this simple necessary condition is in fact sufficient. Our main result is the following.

Theorem 1.2. *Let $E \subset \mathbb{F}_q^d$. Suppose that $|E| > q^k$, $1 \leq k \leq d - 1$. Let H_{k+1} denote a $k + 1$ -dimensional sub-space of \mathbb{F}_q^d . Then $\mathcal{D}(H_{k+1}) \subset \mathcal{D}(E)$. In particular, if $|E| > q^{d-1}$, every possible direction is determined.*

Remark 1.3. It is reasonable to conjecture that if $|E| = q^k$, then $|\mathcal{D}(E)| \gtrsim q^{k-1}$ unless E is of the form $x + H_k$, where H_k is a k -dimensional sub-space of \mathbb{F}_q^d . We are unable to resolve this issue at the moment, though Freiman theorem type consideration (see [9], [10]) should shed some light on the situation. We hope to address this point in a subsequent paper.

Theorem 1.2 is in general best possible as we note above. However, if the set is sufficiently "random", we can obtain stronger conclusions. One reasonable measure of randomness of a set is via the size of its Fourier coefficients. Let χ denote a non-trivial principal character on \mathbb{F}_q . See [6] for a thorough description of this topic.

¹Here and throughout, $X \lesssim Y$ means that there exists $C > 0$, independent of q , such that $X \leq CY$.

Note that if q is prime, we can take $\chi(t) = e^{\frac{2\pi it}{q}}$. The basic properties of characters are the facts that $\chi(0) = 1$, $|\chi(t)| = 1$, where $|\cdot|$ denotes complex modulus and

$$(1.2) \quad q^{-1} \sum_{a \in \mathbb{F}_q} \chi(at) = \delta_0(t),$$

where $\delta_0(t) = 1$ if $t = 0$ and 0 otherwise. Given $f : \mathbb{F}_q^d \rightarrow \mathbb{C}$, define the Fourier transform of f ,

$$\widehat{f}(m) = q^{-d} \sum_{x \in \mathbb{F}_q^d} \chi(-x \cdot m) f(x).$$

We shall also make use of the Plancherel formula

$$(1.3) \quad \sum_m |\widehat{f}(m)|^2 = q^{-d} \sum_x |f(x)|^2.$$

We are now ready to define the notion of randomness we are going to use.

Definition 1.4. We say that $E \subset \mathbb{F}_q^d$, $d \geq 2$, is a *Salem set* if

$$(1.4) \quad |\widehat{E}(m)| \lesssim q^{-d} \sqrt{|E|} \text{ for } m \neq (0, \dots, 0).$$

See [5] for this definition and examples of Salem sets in \mathbb{F}_q^d . See also [13] where the original version of the concept, in the context of measures in Euclidean space is described.

Our second result is the following.

Theorem 1.5. *Suppose that $E \subset \mathbb{F}_q^d$, $d \geq 2$, is a Salem set.*

i) *If $|E| > q^{d-1}$, then $\mathcal{D}(E) = \mathcal{D}(\mathbb{F}_q^d)$.*

ii) *If $|E| \leq q^{d-1}$,*

$$|\mathcal{D}(E)| \gtrsim \min \left\{ \frac{|E|^2}{q}, q^{d-1} \right\}.$$

iii) *If $|E| \leq q^{d-1}$, then*

$$|\mathcal{D}(E)| \gtrsim |E|.$$

In particular, if $|E| \gtrsim q^{\frac{d}{2}}$, $|\mathcal{D}(E)| \gtrsim q^{d-1}$. The lower bound in Part ii) is better than the lower bound in Part iii) if $|E| \gtrsim q$.

Remark 1.6. For a related result, see [3], Theorem 2.2. See that paper and also [12] and [11] for a connection between the problem under consideration here and the expansion phenomenon in graphs.

Remark 1.7. Part ii) holds without the assumption that $|E| \leq q^{d-1}$. We simply wish to emphasize the fact that if $|E| > q^{d-1}$, a much stronger conclusion is already available from Theorem 1.2.

Remark 1.8. The proof of Part ii) below does not use the full strength of the Salem assumption (1.4). What is required is a weaker property $|E - E| \gtrsim \min\{|E|^2, q^d\}$, which follows from (1.4) as Lemma 3.1 shows. To construct a set satisfying this weaker property which is not Salem, just construct a Salem set (see e.g. [5]) on \mathbb{F}_q^k , $k < d$, and embed this \mathbb{F}_q^k as a sub-space of \mathbb{F}_q^d .

Remark 1.9. We note that the conclusion of Theorem 1.5 does not in general hold if E is not a Salem set. To see this, take $E \subset H_{k+1}$, $1 \leq k \leq \frac{d}{2}$, a $(k+1)$ -dimensional sub-space of \mathbb{F}_q^d . Further suppose that $|E| \approx q^{k+\alpha}$ for some $\alpha > 0$. Since $E \subset H_{k+1}$, $|\mathcal{D}(E)| \leq q^k$. Therefore, it is not true that $|\mathcal{D}(E)| \gtrsim \frac{|E|^2}{q}$ since $q^{2k+2\alpha-1}$ is much greater than q^k when q is large if $k \geq 1$. It is also not true in this case that $|\mathcal{D}(E)| \gtrsim |E|$ since $q^{k+\alpha}$ is much greater than q^k when q is large.

Remark 1.10. What we do not know is to what extent Theorem 1.5 can be improved. For example, we do not know of a single Salem subset E of \mathbb{F}_q^d of size $> Cq^{\frac{d-1}{2}}$ for which

$$|\mathcal{D}(E)| = o(q^{d-1})^2.$$

It is reasonable to conjecture that if E is Salem and $|E| \geq Cq^{\frac{d-1}{2}}$, with a sufficiently large constant $C > 0$, then $\mathcal{D}(E) = \mathcal{D}(\mathbb{F}_q^d)$. We do not currently know how to approach this question.

2. PROOF OF THEOREM 1.2

By rotating the coordinates, if necessary, we may define $\nu_E(t_1, \dots, t_k)$ by the expression

$$|\{(x, y) \in E \times E : x_2 - y_2 = t_1(x_1 - y_1), \dots, x_{k+1} - y_{k+1} = t_k(x_1 - y_1); x \neq y\}|.$$

Let χ denote a non-trivial principal additive character on \mathbb{F}_q . It follows from (1.2) that

$$\begin{aligned} \nu_E(t_1, \dots, t_k) &= \sum_{\{(x, y) : (x_2 - y_2) = t_1(x_1 - y_1), \dots, (x_{k+1} - y_{k+1}) = t_k(x_1 - y_1); x \neq y\}} E(x)E(y) \\ &= q^{-k} \sum_{s_1, \dots, s_k \in \mathbb{F}_q} \sum_{x \neq y \in \mathbb{F}_q^d} E(x)E(y) \chi(s_1((x_2 - y_2) - t_1(x_1 - y_1))) \dots \chi(s_k((x_{k+1} - y_{k+1}) - t_k(x_1 - y_1))) \\ &= \frac{|E|(|E| - 1)}{q^k} \end{aligned}$$

²Recall that $X = o(Y)$ for quantities X and Y depending on the parameter q , if $\frac{X}{Y} \rightarrow 0$ as $q \rightarrow \infty$

$$\begin{aligned}
& -q^{-k} \sum_{(s_1, \dots, s_k) \neq (0, \dots, 0)} \sum_{x=y \in \mathbb{F}_q^d} E(x)E(y) \chi(s_1((x_2-y_2)-t_1(x_1-y_1))) \dots \chi(s_k((x_{k+1}-y_{k+1})-t_k(x_1-y_1))) \\
& + q^{-k} \sum_{(s_1, \dots, s_k) \neq (0, \dots, 0)} \sum_{x,y \in \mathbb{F}_q^d} E(x)E(y) \chi(s_1((x_2-y_2)-t_1(x_1-y_1))) \dots \chi(s_k((x_{k+1}-y_{k+1})-t_k(x_1-y_1))) \\
(2.1) \quad & = \frac{|E|(|E|-1)}{q^k} - |E| \left(\frac{q^k-1}{q^k} \right) + R(t_1, \dots, t_k).
\end{aligned}$$

Lemma 2.1. *With the notation above, $R(t_1, \dots, t_k) \geq 0$.*

To prove the lemma, we see that by the definition of the Fourier transform, we see that $R(t_1, \dots, t_k)$ equals

$$\begin{aligned}
& q^{2d-k} \sum_{(s_1, \dots, s_k) \neq (0, \dots, 0)} \widehat{E}(s_1 t_1 + \dots + s_k t_k, -s_1, \dots, -s_k, \vec{0}) \widehat{E}(-s_1 t_1 - \dots - s_k t_k, s_1, \dots, s_k, \vec{0}) \\
& = q^{2d-k} \sum_{(s_1, \dots, s_k) \neq (0, \dots, 0)} \widehat{E}(s_1 t_1 + \dots + s_k t_k, -s_1, \dots, -s_k, \vec{0}) \overline{\widehat{E}(s_1 t_1 + \dots + s_k t_k, -s_1, \dots, -s_k, \vec{0})} \\
& = q^{2d-k} \sum_{(s_1, \dots, s_k) \neq (0, \dots, 0)} |\widehat{E}(s_1 t_1 + \dots + s_k t_k, -s_1, \dots, -s_k, \vec{0})|^2 \geq 0.
\end{aligned}$$

This completes the proof of Lemma 2.1. It follows that

$$\nu_E(t_1, \dots, t_k) \geq \frac{|E|(|E|-1)}{q^k} - |E| \left(\frac{q^k-1}{q^k} \right).$$

The right hand side is positive as long as $|E| > q^k$ and this completes the proof.

3. PROOF OF THEOREM 1.5

Part i) follows instantly from Theorem 1.2. To prove Part iii), we observe that by (2.1) above, we have

$$\nu_E(t_1, \dots, t_{d-1}) = \frac{|E|(|E|-1)}{q^{d-1}} - |E| \left(\frac{q^{d-1}-1}{q^{d-1}} \right) + R(t_1, \dots, t_{d-1}).$$

If $|E| \leq q^{d-1}$,

$$\begin{aligned}
\nu_E(t_1, \dots, t_{d-1}) & \leq 2|E| + R(t_1, \dots, t_{d-1}) \\
& \lesssim 2|E| + q^{d+1} \cdot q^{d-1} \cdot q^{-2d}|E| = |E|,
\end{aligned}$$

where the second inequality holds by the Salem property (1.4). It follows that

$$|E|^2 - |E| \leq \sum_{t_1, \dots, t_{d-1}} \nu_E(t_1, \dots, t_{d-1}) \lesssim |\mathcal{D}(E)| \cdot |E|.$$

We conclude that

$$|\mathcal{D}(E)| \gtrsim |E|$$

and Part iii) is proved.

To prove Part ii), we need the following observation.

Lemma 3.1. *Suppose that $E \subset \mathbb{F}_q^d$, $d \geq 2$, is a Salem set. Then*

$$(3.1) \quad |E - E| \gtrsim \min\{|E|^2, q^d\}.$$

To prove the lemma, define the function $\mu(z)$ by the relation

$$(3.2) \quad \sum_{z \in \mathbb{F}_q^d} f(z) \mu(z) = \sum_{x, y} f(x - y) E(x) E(y).$$

Equivalently, one can set

$$\mu(z) = \sum_{x-y=z} E(x) E(y)$$

and check that

$$\sum_z f(z) \mu(z) = \sum_z f(z) \sum_{x-y=z} E(x) E(y) = \sum_{x, y} f(x - y) E(x) E(y).$$

Observe that $\mu(z) \neq 0$ precisely when $z \in E - E$. Taking $f(z) = \chi(-z \cdot m) q^{-d}$ in (3.2), we see that

$$\widehat{\mu}(m) = q^{-d} \sum_{x, y} \chi((x - y) \cdot m) E(x) E(y) = q^d |\widehat{E}(m)|^2.$$

Applying (3.2) once again with $f(z) = 1$, we get

$$\sum \mu(z) = |E|^2.$$

It follows that

$$\begin{aligned} |E|^4 &= \left(\sum_z \mu(z) \right)^2 \leq |E - E| \cdot \sum_z \mu^2(z) \\ &= |E - E| \cdot q^d \cdot \sum_m |\widehat{\mu}(m)|^2 \\ &= |E - E| \cdot q^{3d} \cdot \sum_m |\widehat{E}(m)|^4 \\ &= |E - E| \cdot q^{3d} \cdot q^{-4d} \cdot |E|^4 \\ &\quad + |E - E| \cdot q^{3d} \cdot \sum_{m \neq (0, \dots, 0)} |\widehat{E}(m)|^4 \end{aligned}$$

$$\begin{aligned}
&\lesssim |E - E| \cdot q^{-d} \cdot |E|^4 + |E - E| \cdot q^{3d} \cdot q^{-2d} |E| \sum_m |\widehat{E}(m)|^2 \\
&= |E - E| \cdot q^{-d} \cdot |E|^4 + |E - E| \cdot q^{3d} \cdot q^{-2d} \cdot q^{-d} |E|^2 \\
&= |E - E| \cdot q^{-d} \cdot |E|^4 + |E - E| \cdot |E|^2.
\end{aligned}$$

In the fourth line above we used the Salem property (1.4). In the fifth line, we used the Plancherel formula (1.3). We conclude that

$$|E - E| \gtrsim \min\{|E|^2, q^d\},$$

as claimed.

We are now ready to complete the proof of Part ii). By definition of $\mathcal{D}(E)$ (1.1), at most q points of $E - E$ account for a given element of $\mathcal{D}(E)$. It follows that

$$|\mathcal{D}(E)| \gtrsim \frac{|E|^2}{q}$$

and the proof of Part ii) is complete.

REFERENCES

- [1] J. Bourgain, N. Katz, and T. Tao, *A sum-product estimate in finite fields, and applications*, Geom. Funct. Anal. **14** (2004), 27-57. [1](#)
- [2] Z. Dvir, *On the size of Kakeya sets in finite fields*, J. Amer. Math. Soc. **22** (2009), no. 4, 1093-1097. [1](#)
- [3] D. Hart, L. Li, C. Y. Shen, *Fourier analysis and expanding phenomena in finite fields*, (<http://arxiv.org/pdf/0909.5471>). [3](#)
- [4] D. Hart, A. Iosevich, D. Koh and M. Rudnev, *Averages over hyperplanes, sum-product theory in vector spaces over finite fields and the Erdos-Falconer distance conjecture*, (accepted for publication by Transaction of the AMS), arXiv:0707.3473, (2007). [1](#)
- [5] A. Iosevich and M. Rudnev, *Erdős distance problem in vector spaces over finite fields*, Trans. Amer. Math. Soc. **359** (2007), no. 12, 6127-6142. [3](#), [4](#)
- [6] R. Lidl and G. Niederreiter, *Finite fields*, Second edition, Cambridge University Press, (1997). [2](#)
- [7] J. Pach and M. Sharir *Geometric incidences*, Towards a theory of geometric graphs, 185-223, Contemp. Math., **342**, Amer. Math. Soc., Providence, RI, (2004). [1](#)
- [8] J. Pach, R. Pinchasi, M. Sharir *Solution of Scott's problem on the number of directions determined by a point set in 3-space*, Discrete Comput. Geom. **38** (2007), no. 2, 399-441. [1](#)
- [9] I. Z. Ruzsa, *An analog of Freiman's theorem in groups. Structure theory of set addition*, Astérisque **258** (1999), 323-326. [2](#)
- [10] T. Sanders, *A note on Freiman's theorem in vector spaces*, Combin. Probab. Comput. **17** (2) (2008), 297-305. [2](#)
- [11] T. Tao and V. Vu, Additive Combinatorics, Cambridge University Press (2006). [1](#), [3](#)
- [12] V. Vu, *Sum-product estimates via directed expanders*, Math. Res. Lett. **15** (2008), no. 2, 375-388. [1](#), [3](#)
- [13] T. Wolff, *Lectures on harmonic analysis*. With a foreword by Charles Fefferman and preface by Izabella Laba. Edited by Laba and Carol Shubin. University Lecture Series, **29**, American Mathematical Society, Providence, RI, (2003). [3](#)

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ROCHESTER, ROCHESTER, NY
E-mail address: iosevich@math.rochester.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MISSOURI, COLUMBIA, MO
E-mail address: hmm5x7@mizzou.edu